


Electronic crypto-memory module

Patent Number: DE3340582
Publication date: 1985-05-23
Inventor(s): BITZER WOLFGANG DIPL ING (DE)
Applicant(s):: ANT NACHRICHTENTECH (DE)
Requested Patent: ☐ DE3340582
Application Number: DE19833340582 19831110
Priority Number(s): DE19833340582 19831110
IPC Classification: G09C1/00 ; H04L9/04 ; H04K1/00
EC Classification: G09C1/10, H04L9/22
Equivalents: ☐ CH665298, ☐ NL8403416, NO167177B, NO167177C, NO844486

Abstract

The invention relates to a crypto-memory module (1) having a data memory (2) which can be loaded and deleted electrically from the exterior, and a crypto-generator (3). The data memory has an external input (6) for loading, but no output for reading its contents outside the crypto-memory module. 

Data supplied from the **esp@cenet** database - I2



DEUTSCHES
PATENTAMT

⑳ Aktenzeichen: P 33 40 582.4
㉔ Anmeldetag: 10. 11. 83
㉕ Offenlegungstag: 23. 5. 85

DE 3340582 A1

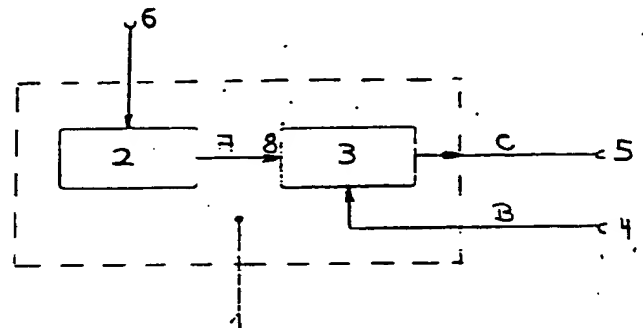
㉗ Anmelder:
ANT Nachrichtentechnik GmbH, 7150 Backnang, DE

㉘ Erfinder:
Bitzer, Wolfgang, Dipl.-Ing., 7153 Weissach im Tal,
DE

Behördeneigentum

㉙ Elektronischer Schlüsselspeichermodul

Die Erfindung betrifft einen Schlüsselspeichermodul (1) mit einem von außen elektrisch ladbaren und löschbaren Datenspeicher (2) und einem Schlüsselgenerator (3). Der Datenspeicher besitzt einen externen Eingang (6) zum Laden, jedoch keinen Ausgang zum Auslesen seines Inhaltes außerhalb des Schlüsselspeichermoduls.



DE 3340582 A1

ORIGINAL INSPECTED

- 1 -

ANT Nachrichtentechnik GmbH
Gerberstraße 33
D-7150 Backnang

BK 83/143
E7/Sch/ht

Patentansprüche:

1. Schlüsselspeichermodul (1), dadurch gekennzeichnet, daß er einen von außen elektrisch ladbaren und löschbaren Datenspeicher (2) enthält und einen Schlüsselgenerator (3) aufweist, der mittels Daten (A) aus diesem Datenspeicher (2) und von außen direkt zuführbaren Daten (B) voreinstellbar ist und daß Ausgang (5) vorhanden ist, über den ein von diesem Schlüsselgenerator (3) erzeugter Grundschlüssel (C) einem angeschlossenen Schlüsselgerät zuführbar ist, wobei der Datenspeicher (2) einen externen Eingang (6) zum Laden desselben, aber keinen Ausgang zum Auslesen seines Inhalts außerhalb des Schlüsselspeichermoduls (1) aufweist.
2. Schlüsselspeichermodul nach Anspruch 1, dadurch gekennzeichnet, daß der Datenspeicher (2) in mehrere Speicherbereiche (a, b ... f) aufgeteilt ist, die von außen adressierbar sind (7 Fig. 2).

3. Schlüsselspeichermodul nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Inhalt eines Speicherbereiches (a, b, ... f) des Datenspeichers nach einer vorgegebenen Anzahl von n Auslesevorgängen gelöscht wird, wobei $n \geq 1$ ist.
4. Schlüsselspeichermodul nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Datenspeicher (2) durch ein RAM mit einer Stromversorgung durch eine eingebaute Batterie realisiert ist.
5. Schlüsselspeichermodul nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß als Schlüsselgenerator (3) ein Blockchiffriergenerator verwendet wird, wobei die Daten A aus dem Datenspeicher (2) dem Schlüsselgeneratoreingang und die von außen direkt zuführbaren Daten (B) dem Klar- bzw. Geheimtexteingang zugeführt werden und der am Ausgang (5) abgegebene Grundschlüssel (C) dem Geheim- bzw. Klartextausgang entnommen wird.
6. Schlüsselspeichermodul nach Anspruch 5, dadurch gekennzeichnet, daß die dem Datenspeicher (2) entnommenen Daten (A) und die von außen zugeführten Daten (B) den beiden Eingängen 8,9 des Schlüsselgenerators (3) in vermischter Reihenfolge zugeführt werden und/oder auch teilweise vorher zueinander addiert werden (modulo 2).

Elektronischer Schlüsselspeichermodul

Zur Verschlüsselung von Daten oder Sprache verwendete elektronische Schlüsselgeräte benötigen als geheimes Element einen sogenannten Grundschlüssel.

Dieser Grundschlüssel wird bei modernen Schlüsselgeräten über eine elektrische oder optische Schnittstelle eingegeben und in einem elektronischen Speicher gespeichert und/oder zur Voreinstellung des Schlüsselalgorithmus verwendet.

Zum Transport und zur Eingabe der Schlüssel können unterschiedliche Datenträger und Eingabegeräte verwendet werden, z.B. Lochstreifen und Lochstreifenleser. In zunehmendem Maße werden hierzu elektronische, tragbare Speichermodule verwendet, in denen der oder die Schlüssel in z.B. RAM-Speichern abgespeichert sind, die durch eine Batterie gepuffert sind. Diese Speichermodule können nun an das mit einem oder mehreren Schlüsseln zu ladende Schlüsselgerät angesteckt werden, um den Schlüssel über die so hergestellte Verbindung zu übergeben.

Da der/die Grundschlüssel das wichtigste Geheimelement in der Schlüsseltechnik darstellen, ist es wichtig, einen Mißbrauch bzw. Verrat der gespeicherten Schlüssel zuverlässig zu verhindern.

Heute versucht man dies im allgemeinen durch organisatorische Maßnahmen zu erreichen: Man betraut mit der Überbringung des Schlüsselmaterials nur besonders verpflichtetes, vertrauenswürdigen Personal.

Besser wäre es natürlich, ein Verfahren zu finden, das einen Verrat des Schlüsselmaterials während des Transports mit technischen Mitteln, unabhängig von der Zuverlässigkeit des Personals, verhindert.

Ein Diebstahl des kompletten mit den geheimen Schlüsseln geladenen Schlüsselmoduls würde sofort bemerkt werden, da er in diesem Falle nicht beim Empfänger eintrifft. Die Schlüssel würden dann gar nicht benutzt werden und wären somit für den Dieb wertlos.

Eine andere Möglichkeit, die Schlüssel zu stehlen, wäre aber, sie während des Transportes mittels einer geeigneten Hilfseinrichtung aus dem Speichermodul zu kopieren. Auch eine Einrichtung in dem Schlüsselspeichermodul, die ein mehrmaliges Auslesen eines Schlüssels verhindert, indem sie diesen nach der Ausgabe im Speicher sofort löscht, bietet hier keine wesentlich erhöhte Sicherheit: Der Dieb könnte die kopierten Schlüssel wieder in den Schlüsselspeichermodul zurückschreiben oder einen gleichaussehenden und gleich funktionierenden Schlüsselspeichermodul mit den gestohlenen Schlüsseln laden und dem rechtmäßigen Empfänger zukommen lassen.

Aufgabe der Erfindung ist es daher, die Möglichkeit, den Inhalt eines Schlüsselspeichermoduls zu kopieren, mit technischen Mitteln sicher zu verhindern.

In den Figuren 1 und 2 ist dies schematisch dargestellt. Der Schlüsselspeichermodul ist mit 1 bezeichnet. Er enthält den Datenspeicher 2 und den angeschlossenen Schlüsselgenerator 3. Die Schlüsselgeneratorvoreinstellung erfolgt über von außen direkt zuführbare Daten B über den Eingang 4 in Verbindung mit aus dem Datenspeicher 2 entnommenen Daten A, die dem Schlüsselrechner 3 über den Eingang 8 zuführbar sind. Der Schlüsselgenerator 3 besitzt einen Ausgang 5, über den ein vom Schlüsselgenerator 3 erzeugter Grundschlüssel C einem angeschlossenen Schlüsselgerät zugeführt wird. Der Datenspeicher 2 hat einen externen Eingang 6 zum Laden; es ist jedoch kein Ausgang zum Auslesen seines Inhalts außerhalb des Schlüsselspeichermoduls 1 vorhanden. Der Datenspeicher 2 kann in mehrere Speicherbereiche a, b ... f aufgeteilt sein, die von

außen über den Eingang 7 adressierbar sind. Man wird den Speicher vorzugsweise so gestalten, daß sein Inhalt nach einer vorgegebenen Anzahl $n \geq 1$ Auslesevorgängen automatisch gelöscht wird. Als Speicher eignet sich ein sogenannter RAM mit Stromversorgung durch eine eingebaute Batterie. Als Schlüsselgenerator 3 dient ein Blockchiffriergenerator, der vorzugsweise als DES (vgl. Nat. Bur. Stand. (US) Fed. Info. Process. Stand. Publ. (FIPS PUB) 46, 17 Pages (1977, Jan. 15)) ausgebildet ist. Man kann die dem Datenspeicher 2 entnommenen Daten A und die von außen zugeführten Daten B den beiden Eingängen 4,8 des Schlüsselgenerators 3 in vermischter Form zuführen und/oder vorher zueinander addieren (modulo 2).

Durch die Europäische Patentschrift 22 069 ist es zwar bereits bekannt, den Schlüsselspeichermodule (dort "Schlüsselbehälter" genannt) mit einer Quarzuhr auszurüsten, die die Schlüssel nur während bestimmter "Zeitfenster" zum Auslesen freigibt und somit ein unberechtigtes Auslesen der gespeicherten Schlüssel vor der vorbestimmten Zeit verhindert.

Dies hat jedoch einige Nachteile, vor allem, daß die abgespeicherten Schlüssel nur zu den vorgegebenen Zeitpunkten verwendet werden können. Die Speichermodule können somit nicht "auf Vorrat" geladen und bereitgelegt werden. Dies erfordert aufwendige organisatorische Maßnahmen. Bei dem erfindungsgemäßen Verfahren bzw. der erfindungsgemäßen Schaltungsanordnung werden diese Nachteile vermieden.

Der Grundgedanke der Erfindung besteht dabei darin, daß der Schlüsselspeichermodule niemals seinen eigentlichen Speicherinhalt direkt ausgeben kann, sondern daß ein auszugebender Grundschlüssel erst bei Abruf durch das zu ladende Schlüsselgerät durch einen in den Schlüsselspeichermodule integrierten Schlüsselgenerator aus einem

im Schlüsselmodul gespeicherten geheimen "Quellschlüssel" und einem von dem zu ladenden Schlüsselgerät dem Schlüssel-speichermodul zugeführten "Zusatzschlüssel" berechnet wird. Eine Entschlüsselung eines Kryptogrammes ist somit nur möglich, wenn beim Empfänger derselbe Grundschlüssel und, um dies zu erreichen, derselbe Quellschlüssel und Zusatzschlüssel vorliegt, wie beim Absender. Der Quellschlüssel läßt sich nicht auslesen und damit nicht von einem Dieb kopieren. Der Zusatzschlüssel wird erst erzeugt, wenn sichergestellt ist, daß der Schlüsselspeichermodul beim rechtmäßigen Empfänger angekommen ist. Der Dieb hat damit auch keine Möglichkeit, sich schon im Voraus einen später verwendeten Grundschlüssel ausgeben zu lassen. Wenn der Zusatzschlüssel aus z.B. 30 Bit besteht, so ist die Wahrscheinlichkeit, daß der Dieb durch Ausprobieren zufällig an einen richtigen Grundschlüssel kommt gleich 2^{-30} oder kleiner als 10^{-10} .

Der Zusatzschlüssel kann dabei bei der Erstellung eines Kryptogramms mittels eines Zufallsbitfolgengenerators erzeugt und zusammen mit dem Kryptogramm dem Empfänger übertragen werden. Es kann hierzu auch der ohnehin bei den meisten Schlüsselgeräten benötigte "Spruchschlüssel" oder "initialising variable" mitverwendet werden.

20015

NACHGEREICHT

Nummer:

33 40 582

Int. Cl. 3:

G 09 C 1/00

Anmeldetag:

10. November 1983

Offenlegungstag:

23. Mai 1985

HT

- 7 -

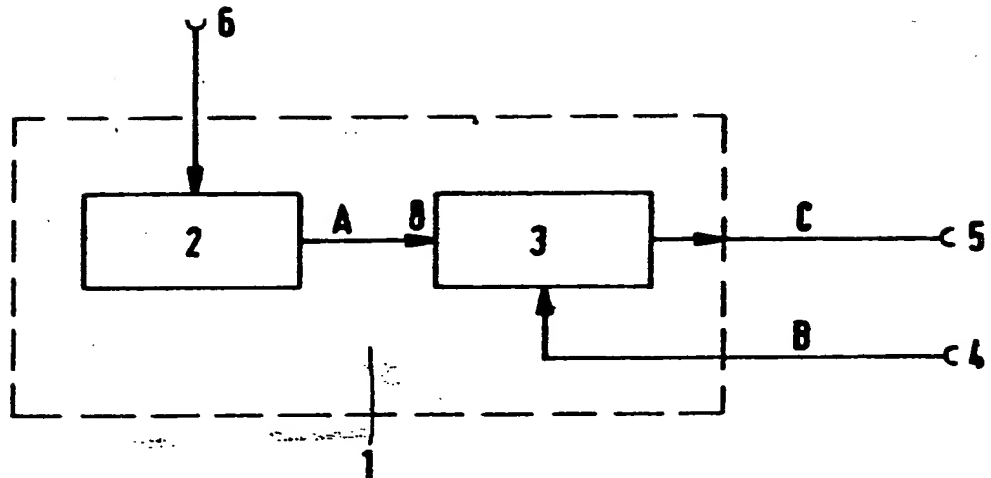


FIG. 1

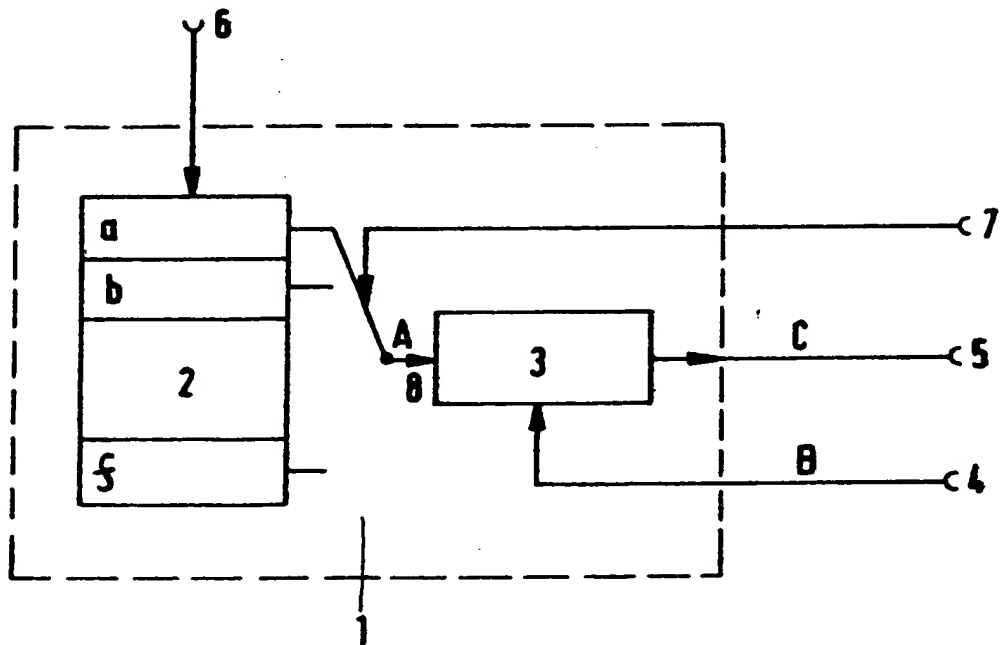


FIG. 2